The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/14/2017

SUBJECT:
Cumulative Security Update for Internet Explorer (MS17-006)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Internet Explorer, the most severe of which could allow for remote code execution if a user views a specially crafted web page. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There has been a report of a memory corruption vulnerability (CVE-2017-0149) being exploited in the wild.

SYSTEMS AFFECTED:
- Internet Explorer 9, 10, 11

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Internet Explorer, the most severe of which could allow for remote code execution if a user views a specially crafted web page. Details of these vulnerabilities are as follows:

- Three remote code execution vulnerabilities exist when Microsoft Browsers improperly access objects in memory. (CVE-2017-0018, CVE-2017-0037, CVE-2017-0149)
- Two remote code execution vulnerabilities exist in the way that the JScript and VBScript engines render when handling objects in memory. (CVE-2017-0040, CVE-2017-0130)

- Three information disclosure vulnerabilities exist in the way Internet Explorer handle objects in memory. (CVE-2017-008, CVE-2017-009, CVE-2017-0059)
- Two spoofing vulnerabilities exist when a Microsoft browser does not properly parse HTTP responses. (CVE-2017-0012, CVE-2017-0033)
- One information disclosure vulnerability exists when the JScript scripting engine does not properly handle objects in memory. (CVE-2017-0049)
- One elevation of privilege vulnerability exists when Internet Explorer does not properly enforce cross-domain policies. (CVE-2017-0154)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches by Microsoft immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Microsoft:
https://technet.microsoft.com/library/security/MS17-006

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0008
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0009
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0012
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0018
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0033
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0037
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0040
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0049
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0059
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0130
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0149
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0154